```
=> d his

     (FILE 'USPAT' ENTERED AT 11:24:27 ON 11 SEP 1999)
L1             1 S 4472790/PN
L2        561688 S USER# OR OPERATOR#
L3             1 S L1 AND L2
L4            74 S (OVERRID? OR OVER RID?)(6A)(SECUR? OR PROTECT?)(10A)(USE
R#
```

US PAT NO: 5,925,126 [IMAGE AVAILABLE] L4: 3 of 74
TITLE: Method for security shield implementation in computer system's software

DETDESC:

DETD(9)

For example, in both UNIX and NT systems, a "Superuser" power program **overrides** all other system **protections**. The "Superuser" was designed to give one class of **user** absolute control over system administration activities and, in large organizations, this capability is typically assigned to many people. Superusers may remove any or all access controls, violate security policies, view and change any file, read anyone's e-mail, and remove passwords. Security in such software systems becomes an exponentially complex and expensive task in the presence of Superuser because all resources must be secured, monitored, and controlled against inadvertent Superuser attacks, as seen in FIG. 3. In addition to files 48 owned by the user, shared files 50 which are not sensitive, and shared files 52 which are sensitive, programs. operator commands, systems and network services are all vulnerable to Superuser threat and, therefore, must be protected.

US PAT NO: 5,923,843 [IMAGE AVAILABLE] L4: 5 of 74
TITLE: Method and apparatus for overriding access security to a PC when a password is lost

SUMMARY:

BSUM(10)

The present invention allows a user to regain access to a TV/PC or other computing device in the event that user selected passcode information is forgotten or inadvertently changed to an unknown value by providing the **user** with a mechanism to enter access **security override** passcode information. To effectuate the **override** mechanism of the present invention while still restricting access to authorized users, the present invention provides that such override passcode information be resident on a medium used by a data input device connected to the computing device and that the medium be read by the security device to obtain the override passcode information. For example, the override passcode information may be resident on a compact disk and a compact disk drive is used to input the override passcode information. In such a case, the user can retain physical possession of the medium containing the override passcode information in a manner akin to having a master key which can be used when a custom key is lost.

DETDESC:

DETD(6)

To activate the override mechanism of the present invention, the local security device 18 is programmed to allow the user, when the local security device 18 is in the secured mode, to request that the local **security** device 18 enter an **override** mode. Upon entering the override mode, the **user** is either instructed to place the medium containing the override passcode information in the corresponding input device, or alternatively, is allowed to select which input device is to be used to enter the override passcode information. The local security device 18 then reads the override passcode information and verifies that i

US PAT NO: 5,768,373 [IMAGE AVAILABLE] L4: 12 of 74
TITLE: Method for providing a secure non-reusable one-time password

SUMMARY:

BSUM(10)

Thus, it is desirable to develop a system which allows a user to gain access to his/her computer data even if the user has forgotten the password. However, because data security is of prime significance to users who use passwords, it is also desirable to allow a **user** to **override** password **protection** to data in a way that does not significantly compromise the security of the data.

U

US PAT NO: 5,729,734 [IMAGE AVAILABLE] L4: 16 of 74
TITLE: File privilege administration apparatus and methods

DETDESC:

DETD(27)

In one embodiment, the administrator can check the box entitled "Enable access to the item" 421. This command is an **overriding security** feature that, when checked, allows any **user** access to the selected items. This security feature provides the administrator the assurance of knowing that a specific item will not be accessed by a selected user unless this box is checked. In FIG. 5, if box 421 is not checked, i.e., the box does not contain an "X", the general access privileges assigned to all users, including the one in box 431, will be ignored.

US PAT NO: 5,128,996 [IMAGE AVAILABLE] L4: 38 of 74
TITLE: Multichannel data encryption device

DETDESC:

DETD(243)

When selected, the options sub-menu displays each option available to the user, and the right-hand portion of the display shows the currently entered value for each option. The menu option "Ability To Quit" allows the user to quit the application and return to the operating system in disk-based systems and may be deleted in ROM-based systems. The menu function "Configure" activates another sub-menu discussed further below. The menu function "Status Interval" controls the number of seconds between display updates. The menu function "Sample Interval" controls the number of hours between updating the total fields for threshold checking. The menu function "Threshold Values" controls percentage values for activating an alarm. The menu function "Idle Timeout" controls a time, set in minutes, for controlling the amount of time the keyboard is idle before the system reverts to the main status screen and resetting the user level to level zero. This feature prevents an unattended unit from remaining at a high user level, thus providing access to sensitive key information. The menu function "Check Digit Length" controls the number of check digits to verify, thus providing compatibility with a number of alternate system configurations. The menu function "Key Parts" controls the number of key segments prompted for during key entry and can be any value from one to nine. The menu function "Table Parts" controls the number of parts entered in a Diebold table entry sequence. The menu function "New Password" allows the user to specify passwords for each **user** level. The menu function "Password **Protect**" allows **users** to **override** the system password **protection** scheme for servicing and may be deleted in secure systems.

```
=> d his

     (FILE 'USPAT' ENTERED AT 10:38:20 ON 11 SEP 1999)
L1        444426 S TIME(5A)(FRAME# OR PERIOD#)
L2           245 S (TIMES OR NUMBER#)(6A)ACCESS?(6A)(ATTEMPT# OR TRY#)
L3            42 S L1(P)L2
L4           204 S OVERRIDE?(6A)(SECUR?)
L5           410 S 711/163,164/CCLS
L6             1 S L4 AND L5
```

US PAT NO: 5,793,972 [IMAGE AVAILABLE] L3: 8 of 42
TITLE: System and method providing an interactive response to direct mail by creating personalized web page based on URL provided on mail piece

CLAIMS:

CLMS(17)

17. The system as defined in claim 16, wherein the access database generating means comprises means for determining the **number** of unauthorized **access attempts** associated with an Internet protocol address within a determined **period** of **time**.

CLAIMS:

CLMS(18)

18. The system as defined in claim 17, wherein the access means is coupled to the unauthorized attempts access database for denying access to a remote computer having an Internet protocol address for which more than a specified **number** of unauthorized **access attempts** have been recorded within a determined **period** of **time**.

CLAIMS:

CLMS(19)

19. The system as defined in claim 18, wherein the access database generating means comprises means for determining the total **number** of unauthorized **access attempts** within a determined **period** of **time**.

CLAIMS:

CLMS(20)

20. The system as defined in claim 19, wherein the access means is coupled to the access generating database means for denying access to the web server when more than a determined **number** of unauthorized **access attempts** have been recorded within a determined **period**
o

US PAT NO: 5,732,212 [IMAGE AVAILABLE] L3: 13 of 42
TITLE: System and method for remote monitoring and operation of personal computers

DETDESC:

DETD(114)

If no password is received after a pre-set **period** of **time** or an invalid password is received 603, then a "Session" counter is incremented to count the **number** of unsuccessful **access attempts** during a session. If this counter exceeds a user specified limit, the counter is reset to zero, a "Lockout" counter is incremented, a session lockout flag is set, and a data packet is returned to the Remote PC indicating that access to the Host Unit is denied for the session and processing returns to the Process Access Request routine 601. If the "Lockout" counter exceeds a user specified limit, as obtained from non-volatile RAM, no user will be permitted access to the Host Unit until the "Action" button on the front of the Host Unit is pressed.

U

S PAT NO: 5,729,542 [IMAGE AVAILABLE] L3: 14 of 42
TITLE: Method and apparatus for communication system access

SUMMARY:

BSUM(7)

In order to reduce access delay in other wireless systems a number of medium access control (MAC) protocols have been proposed, including both non-contention systems, and well-known contention systems like ALOHA, Slotted-ALOHA, reservation ALOHA, CSMA (Carrier-Sense Multiple Access), DSMA (Digital-Sense Multiple Access), PRMA (Packet Reservation Multiple Access) and QCRA (Queued Contiguous Reservation Aloha). Enhancements to such systems have also been proposed using control algorithms to modify access probabilities. Thus, e.g., pseudo-Bayesian control techniques have been suggested to modify slotted-ALOHA systems based on the **number** of **access attempts** per given **time period**. Using such a technique, a base station might broadcast a persistence value p=.beta./v periodically, where .beta. is a constant and v is an estimate of the current number of ready communication units (e.g., meaning those communication units with data to transmit at that **time** (e.g., a burst **period**)). A ready user transmits an access request with probability p during any available access burst period. Thus a persistence value is a maximum permitted probability of making an access request at a given access opportunity.

DETDESC:

D

US PAT NO: 5,495,235 [IMAGE AVAILABLE] L3: 19 of 42
TITLE: Access control system with lockout

ABSTRACT:
An access control system stores two codes for each user that is authorized to access a resource, a primary code and a secondary code. When a user desiring access inputs the primary code to the system, the code is compared with the stored code for that user. If the primary code is valid, the user is allowed to access the resource. However, if the primary code is entered incorrectly, a count of the number of invalid attempts for that user is incremented, and if the count does not exceed a first threshold, the user can **try** again. When the **number** of invalid **access attempts** for the user exceeds the first threshold, the system requires the user to correctly input both the primary and secondary codes, before access to the resource is allowed. A second count is also maintained of the number of failed attempts in providing both codes. When the number of failed attempts exceeds a second threshold, the user is "locked out", i.e, prevented, from gaining access to the resource for a specified **period** of **time**, even if the correct primary and secondary codes are entered during that period. The arrangement is more convenient than using a single, longer code in a conventional access control system with lock out, because, most of the time, a user only needs the primary code to access the resource. However, even if the first threshold is exceeded, an authorized user can still get access to the resource by correctly inputting both codes. The dual code system reduces the inconvenience caused by authorized users being locked out while also increasing security.

SUMMARY:

BSUM(11)

When the system is in its "primary state" and a user inputs the primary code to the system, the code is compared with the stored code for that user. Under normal circumstances, the primary code is recognized as valid, and the system then allows the user to gain access to the resource. If the primary code is entered incorrectly, a first count "count.sub.-- 1" of the number of invalid attempts for that user is incremented, and if the count does not exceed a first (generally small) threshold value C.sub.1, the user is invited to **try** again. However, once the **number** (count.sub.-- 1) of invalid **access attempts** for the user exceeds the first threshold C.sub.1, the access control system advances to its "extended state" and requires the user to correctly input both the primary and secondary codes, (i.e., the extended code) before access to the resource is allowed. A second count "count.sub. 2" is also maintained of the number of failed attempts in providing the extended code. When the number of failed attempts using the extended code exceeds the second (generally large) threshold C.sub.2, the system advances to the "lockout state" in which the user is "locked out", i.e, prevented, from gaining access to the resource for a specified lockout **time period** T.sub.L, even if the correct extended code is entered during that period.

DETDESC:

DETD(5)

In response to the access request received in step 201, an update process is performed in step 202 in order to determine if counts count.sub.-- 1 and/or count.sub.-- 2 should be reset, and to control the

system state, based upon the time difference between the current time and the time at which the last failed access attempt occurred. Details of the update process are described below in connection with FIG. 3. Next, the information received in step 201 is applied via interface 121 to processor 125, to enable retrieval from database 127 of the previously stored primary and secondary access codes and system state information that are associated with the particular user requesting access. The primary and secondary codes are used for validation in steps 209 and 225. Generally speaking, system state information indicates, for a particular user requesting access, information regarding previous access attempts. Three states are defined: primary, extended and lockout. In the primary state, the particular user requesting access has not made more than a first **number** C.sub.1 of invalid **access attempts** in a first **time period** T.sub.1. At this point, this user can gain access using only the primary code. In the extended state, the particular user requesting access has exceeded the first threshold C.sub.1 by making more than C.sub.1 invalid access attempts during period T.sub.1. However, this particular user has not made more than a second **number** C.sub.2 of invalid **access attempts** in a second **time period** T.sub.2. At this point, the user can gain access using both the primary and secondary access codes. In the lockout state, the particular user requesting access has exceeded the second threshold C.sub.2 by making more than C.sub.2 invalid access attempts during period T.sub.2. At this point, this user cannot gain access to the resource, even if the extended (primary and secondary access codes) are correctly input. The system then remains in the lockout state for a lockout **time period** T.sub.L. The system state information is used in decision steps 204 and 207, as d

US PAT NO: 4,472,790 [IMAGE AVAILABLE] L6: 1 of 1
US-CL-CURRENT: **711/164**; 364/964, 964.2, 969, 969.2, 969.3, DIG.2

ABSTRACT:
The embodiment provides selective supervisory disablement of fetch protection for a special storage subarea (such as for the first half of the first 4KB block) while fetch protection is enabled for an area containing the subarea by a single storage protect key. That is, the fetch protect for the subarea (normally provided in the fetch protect for the entire area) by the area's protect key is overriden by the selective subarea disablement control, so that accesses to the subarea are not fetch protected by the storage key. The **override** protection control is **secured** by its enablement via a field position in a control register only accessible to supervisory programming. Thus, while fetch protection is set on for a predefined 4KB block, the fetch protect override controls can disable the fetch protection for a portion of the block's real addresses (e.g. addresses 0-2047).